COUNCIL ON FOREIGN RELATIONS

58 EAST 68TH STREET ▪ NEW YORK ▪ NEW YORK 10021

Statement of

Stephen E. Flynn, Ph.D.
Senior Fellow, National Security Studies
Council on Foreign Relations
sflynn@cfr.org
(212) 434-9676

on

"Port and Maritime Security Since September 11, 2001"

presented before the

United States Senate
Committee on Commerce, Science, and Transportation
Charleston Maritime Center
Charleston, South Carolina.

Hearing on
"S. 1214, The Port and Maritime Security Act"

1:30 p.m.
Tuesday, February 19, 2002

Good morning, Mr. Chairman.

My name is Stephen Flynn. I am a Senior Fellow with the National Security Studies Program at the Council on Foreign Relations. I am also a Commander in the U.S. Coast Guard and a professor at the U.S. Coast Guard Academy. Since 1999, I have been conducting research at the Council that has been examining in large part the security weaknesses associated with the system of intermodal transportation that is so indispensable to supportting global trade and travel. That project has afforded me the opportunity to conduct field visits within major seaports throughout the United States, in Montreal, Rotterdam, Hong Kong, and Kingston, Jamaica.

It is privilege for me to be here today to testify on the state of seaport security since the tragic events of September 11 and to outline my views on S. 1214, the Port and Maritime Security Act. In my testimony, I hope to convey two things. First, I will add my voice to those of the other witnesses in validating the overdue government attention and resources now being given to the critical issue of seaport and maritime transportation security. Second, I will make the case for doing what ever can be done to bolster the international and intermodal dimensions of this historic piece of legislation.

Mr. Chairman, I worry that as you pursue this important agenda to advance port and maritime security you are racing against a return to complacency. Rather than recognizing September 11 as a harbinger of how warfare will be waged in the 21st Century, it appears that many Americans are choosing to see it as an aberrant event where, thanks to our impressive counter-terrorist operations overseas, we soon will be largely free to return to our "normal" lives here at home. I hold just the opposite view. I would argue that we are at greater risk precisely because of the example of the catastrophic terrorists acts of September 11. The Al Qeada terrorists who leveled the twin towers and slashed open the Pentagon made it look easy. Also, nineteen men wielding box-cutters ended up accomplishing what no adversary of the world's sole superpower could ever have aspired to: the successful blockade of the U.S. economy that resulted from the rush by federal authorities to close U.S. airspace, shut down the nation's seaports, and slow truck, car, and pedestrian traffic across the land borders with Canada and Mexico to a trickle. They achieved a very big bang for a very small buck! We should expect that America's adversaries have watched and learned.

Americans need to come to grip with three realities. First, there is military value to engaging in acts of catastrophic terrorism. It is not simply about killing people in large numbers or toppling buildings. It is about generating the collateral societal and economic disruption associated with these attacks, thereby weakening the power of the targeted state, and creating a substantial incentive for it to reassess its policies. Disruption is the military objective, not corpses and rubble.

Second, for the foreseeable future, there will be anti-American terrorists with global reach, capable of carrying out catastrophic attacks on U.S. soil, including the use of chemical and biological weapons. Regardless of our current efforts to roll up the Al Qeada network, places will always exist for terrorists to hide, especially before they have committed widespread atrocities, and new adversaries will eventually arise to fill the shoes of those who have perished. As with the war on drugs, calls for "going to the source" may sound good in theory, but it will prove illusive in practice.

Terrorism expert David Long suggests a compelling analogy when he asserts "terrorism is like the flu—there will always be a new strain each season."

Third, many of America's adversaries will find catastrophic terrorism to be their most attractive military option precisely because of the complete dominance the United States possesses across the conventional spectrum of force. If anyone thinks they can succeed in a pitch battle against U.S. armed forces, they should check with the Iraqi Republican Guard or the Taliban army. The only rational option for the adversaries of the world's sole superpower is to conduct asymmetric warfare. And the most attractive asymmetric targets are the civil and economic elements of power precisely because they are the real basis for U.S. power and they are presently largely unprotected.

As I survey the menu of tempting targets against which to conduct a catastrophic terrorist act, I find our seaports and the intermodal transportation system among the most attractive. First, because we start from such a low security baseline as documented by the report of the Interagency Commission on Crime and Security in U.S. Ports that helped spawn S.1214. Inadequate security in our seaports is not simply a result of benign neglect in the face of what was perceived to be a low threat. It is also the cumulative result of what I would call, "malign neglect." Many in the maritime transportation industry, struggling in the face of competitive pressures for greater efficiencies and lower costs, actively resisted expenditures on security that would erode their already razor-thin profit margins. Prior to September 11, the general neglect of America's seaports, both in terms of investment in public resources and attention from cash-strapped agencies like the Coast Guard and U.S. Customs, translated into a maritime front door that was virtually wide-open. Despite extraordinary efforts made by federal, state, and local officials since 9-11, things are now only marginally better. Seaports remain the only international boundaries that receive no federal funds for security infrastructure—something the Hollings bill properly aims to correct.

The fact that greater vigilance within our seaports has not translated into much in the way of additional security is a reflection of the second reason why I believe seaports like Charleston make attractive targets—ports are part of a global transportation network that can be compromised at the weakest link within that network. Charleston is the fourth largest container port in the United States. More than 40 steamship lines carry U.S. trade between Charleston and 140 countries around the world. 1.5 million containers moved through this port last year that originated from loading docks of tens of thousands of factories or freight forwarders from every continent. At a cost of $1500-$3000, a multi-ton container can be shipped to practically anywhere on the planet. There are no security standards associated with loading a container. There is no requirement that a container be accounted for as it moves from its point of origin, to the port of embarkation. There are not even any agreed upon security guidelines, though there was a discussion begun last week at the International Maritime Organization to begin to tackle that issue. What this translates into is that there are ample opportunities for a terrorist or a criminal to compromise freight shipments destined for U.S. ports. Drugs, arms, and migrant traffickers have been doing this for years.

In short, seaports make great targets because you can essentially launch an attack from a factory, a freight forwarder, or virtually anywhere within the intermodal transportation system, far from

our shores. If the Port of Charleston were to be targeted by a terrorist, there would be plenty of places to hide a weapon among the 12 million tons of cargo, loaded and unloaded in the terminals here in 2001. An adversary could invest in a GPS transponder and track the box's location by satellite and set it off using a remote control. Or he might install a triggering devise that would set the weapon off if the door of the container were opened for examination.

That brings me to my third reason to worry about the vulnerability of the seaports and the intermodal transportation system. If a container were to be used as a poor man's missile and it was set off in a seaport, the inevitable fallout would be to generate concern about the 11.5 million other containers that arrived in the United States last year. How would we know they were bomb free? The answer right now is that we couldn't really say one way or the other with any real confidence, unless we opened and inspected them all. With more than 90 percent of all transoceanic general cargo being shipped in containers to and from the United States, stopping and examining every container would translate into grinding global commerce to a halt. It would make the disruption caused by the anthrax mailings look like a minor nuisance by comparison. When the mail service to Washington was compromised, we switched to using more e-mails, faxes, and FEDEX. If we have to do a security scrub of the intermodal transportation system, there is virtually no alternatively to a box for moving freight. Within day, factories would go idle. As the world's leading importer and exporter, most of the world's economies would share our pain.

Expressed succinctly, seaports and the intermodal transportation system are America's Achilles Heel. This fact has three very important implications for the subject of today's hearing on the vulnerability of U.S. seaports and how the government is structured to the safeguard them:

(1) Seaports cannot be separated from the international transport system to which they belong. Ports are in essence nodes in a network where cargo is loaded on or unloaded from one mode—a ship—to or from other modes—trucks, trains, and, on occasion, planes. Therefore, seaport security must always be pursued against the context of transportation security. In other words, efforts to improve security within the port requires that parallel security efforts be undertaken in the rest of the transportation and logistics network. If security improvements are limited to the ports, the result will be to generate the "balloon effect"; i.e., pushing illicit activities horizontally or vertically into the transportation and logistics systems where there is a reduced chance of detection or interdiction.

(2) Port security initiatives must be harmonized within a regional and international context. Unilateral efforts to tighten security within U.S. ports without commensurate efforts to improve security in the ports of our neighbors will lead shipping companies and importers to "port-shop"; i.e., to move their business to other market-entry points where their goods are cleared more quickly. Thus the result of unilateral, stepped-up security within U.S. ports could well be to erode the competitive position of important America ports while the locus of the security risk simply shifts outside of our reach to Canada, Mexico, or the Caribbean to ports such as Halifax, Montreal, Vancouver, and Freeport.

(3) Since U.S. ports are among America's most critical infrastructure, they should not be viewed as a primary line of defense in an effort to protect the U.S. homeland. It is only as a last resort that we

should be looking to intercept a ship or container that has been co-opted by terrorists is in a busy, congested, and commercially vital seaport.

The bottom line is that while we must put our own house in order, the maritime dimension of the homeland security challenge cannot be achieved at home. It is the international trade corridors that must be secure, not just the off-ramps that bring trade to our shores. S.1214 recognizes this by including a chapter for international port security. But most general cargo does not originate in a port—it starts much further upstream necessitating the need to move toward point of origin controls, supported by a concentric series of checks built into the system at points of transshipment (transfer of cargo from one conveyance to another) and at points of arrival.

A common set of standard security practices to govern the loading and movement of cargo throughout the supply chain must be developed. The goal is to ensure that an authorized shipper knows precisely what is in a shipment destined for U.S. shores and can report those contents accurately. A second objective is to ensure the electronic documentation that goes with the shipment is complete, accurate and secure against computer hackers. A third objective is to reduce the risk of the shipment being intercepted and compromised in transit.

This last objective is best achieved by advancing the means for near-real time transparency of trade and travel flows through technologies that can track the movement of cargo and conveyances and which can detect when freight may have been tampered with. Such a system ideally creates a deterrence for criminals or terrorists to try and intercept and compromise shipments in transit. Greater transparency also enhances the ability for enforcement officials to quickly act on intelligence of a compromise when they receive it by allowing them to pinpoint the suspected freight. The importance of providing the means for intelligence-driven targeting cannot be overstated. The sheer number of travelers and volume of trade along with the possibility of internal conspiracy even among companies and transporters who are deemed low-risk makes critical the ongoing collection of good intelligence about potential breeches in security. But, that intelligence is practically useless if it helps only to perform a post-attack autopsy. Mandating "in-transit accountability and visibility" would provide authorities with the means to detect, track, and intercept threats once they receive an intelligence alert, long before a dangerous shipment entered a U.S. seaport.

S.1214 provides a toehold to advance such a comprehensive approach under section 115, "mandatory advanced electronic information for cargo and passengers and other improved customs reporting procedures"; section 118, "research and development for crime and terrorism prevention and detection technology"; and section 207, "enhanced cargo identification and tracking." If all these sections along with a section 108, "international port security," could be refined to take a more comprehensive systems approach and could be effectively put on steroids during the conference committee process, the Port and Maritime Security Act of 2001 would truly represent a substantial step forward in what promises to be a long and difficult war on global terrorism.

Conclusion:

Building a credible system for detecting and intercepting terrorists who seek to exploit or target our seaports and international transport networks would go a long way towards containing the disruption potential of a catastrophic terrorist act. A credible system would not necessarily have to be perfect, but it would need to be good enough so that when an attack does occur, the public deems it to be as a result of a correctible fault in security rather than an absence of security.

Ultimately getting seaport security right must not be about fortifying our nation at the water's edge to fend off terrorists. Instead, its aim must be to identify and take the necessary steps to preserve the flow of trade and travel that allows the United States to remain an open, prosperous, free, and globally-engaged society.